(d)(2) The Notification message for in-band and out-of-band signaling shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 4: Notification Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber. With the redefinition of subject and subscriber, there was a re-definition of CaseIdentity from its source in J-STD-025.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
Audible Visual or Displayed Signal	M	Identifies the audio signal, visual signal, or displayed text sensed by the Subscriber or Subject. This requirement requires that the telecommunication service provider have knowledge that information was sensed by human beings. This provides a monumental medical and technological challenge, especially if the CALEA requirement for unobtrusive access is to be observed.

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(d)(3) The Notification message for in-band and out-of-band signaling shall adhere to the following ASN.1 syntax definition:

```
Notification :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CallIdentity,
audioVisualDisplay  [4]     VisibleString (SIZE (1..128) )}
```

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

This encoding does not readily differentiate between alphanumeric display information, in-band tones, and out-of-band commands sent toward the subject. Law enforcement may find such distinction useful. It should also be possible to sent multiple indicators with a single message or to report such indicators in existing J-STD-025 messages.

(e) *Timely Delivery of Call-identifying Information.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of expeditiously accessing and delivering call-identifying information to law enforcement contemporaneously with the communications to which it pertains, or in a manner comparable to the speed with which other signaling messages are sent in the public network so that call-identifying information may be associated with the related communications. The following requirements shall apply to the delivery of call-identifying information.

As a general statement, telecommunication service providers and their equipment vendors will attempt to deliver the call-identifying information "as fast as possible," because there is nothing to gain and a lot to lose by delaying these messages. A problem arises in setting the priority of these messages. One solution, which is currently used for delivering call identifying information, is to extract the required information from call detail records for the call. In general this is an inexpensive method for accessing the call identifying information to the extent that it is currently required in J-STD-025. The call detail information requires processing by adjunct processors within the switching system. This processing is done independently of call processing at a somewhat lower priority. As a result some systems may not make this information available until several minutes after a call. Law enforcement would like to have this solution banned even though it meets the requirements of J-STD-025 and is an example of the status quo. [Besides timing, this solution may be rendered deficient and unworkable if some of the capabilities proposed in this proposed rule are adopted.]

This requirement has evolved a little in what law enforcement is asking for. In the past they have requested improved correlation over J-STD-025. J-STD-025 does

provide enough information in its CDC messages to correlate them with the content delivered over a CCC. This is a basic requirement of CALEA.

This general requirement has three separate sets of sub-requirements expanded below: [1] contemporaneous delivery, [2] synchronization between CCC and CDC, and [3] identification tags inserted into the CCC stream. Only the requirements marked with a [1] are required to meet (e). Requirement set [2] is to get additional synchronization markers inserted into the CCC and to synchronize the clocks used for the time stamps on the CDC messages. Requirement set [3] is to insert additional identification tags into the CCC. This is because law enforcement seems unable to make the leap between traditional in-band signaling techniques and modern digital out-of-band signaling techniques. Even though efforts are made to modernize the network and surveillance delivery techniques, law enforcement is insisting using the same dedicated facilities it used in 1967.

The three requirement sets conflict with each other and requirements in J-STD-025. Only one method need to be implemented to state the original "punch list" objective for improved correlation. With the current objective for contemporaneous delivery, neither requirement set [2] nor [3] are necessary.

(e)(1) Each CDC message shall contain a time stamp required to associate and synchronize the message to the call content delivered separately over a CCC. The time stamps shall be generated using the clock of the network element containing the IAP. The time stamp on each of the call event messages shall be accurate within 100 milliseconds (ms) of the triggering events described in J-STD-025 for each message.

In effect this requirement is only requesting that time stamps be accurate to 0.1 seconds since J-STD-025 already has time stamps referenced to network elements generating the time stamps. [This requirement is independent although it leans toward requirement set 2]

(e)(2) The activation of a CCC shall contain an event that marks a change from an idle state to an active state (e.g., the transmission of the time stamp and serial number) that is detectable at the collection function. The CCOpen message time stamp shall mark (within

100 ms) the change in status and shall be the timing reference for synchronization of CDC message times to the CCC call content flow.

The marker should precede the delivery of call content including any in-band call identifying information, however as defined herein, it must follow the in-band call identifying information to meet the 100 ms requirement. Because of this, normal call markers such as an off-hook signaling, alerting signal or call setup message are not acceptable. This seems to require an in-band tone. [Requirement set 2, although there is interaction with requirement set 3]

J-STD-025 already provides for a CCOpen message to mark the change in status and it contains a time stamp.

The last sentence further forces the implementation design by requiring that the CDC CCOpen and CCClose messages be generated by the accessing system itself and not by an adjunct or ancillary support system. Without this requirement the CCOpen and CCClose messages could be generated external to the switching system by converting DC on- and off-hook signaling into the CDC CCOpen and CCClose messages. [Requirement set 2]

The insertion of the marker tones increases the time required to deliver call content and may increase the requirements for capacity in order to not miss content on a series of serial calls made by an intercept subject.

(e)(3) To enable law enforcement to correlate CDC messages with CCC information, call event messages shall be delivered from the IAP to the demarcation point at the carrier facility in as near real time as possible, but no later than three seconds after the occurrence of the associated call event, with a probability of 99%.

This requirement forces electronic surveillance to be at the same or higher priority as call processing within a switching system. [Requirement set 1]

Network traffic engineering is typically designed to handle the fifth busiest busy hour in the year. On a daily basis this works out to a probability of 98% (i.e., 360/365). [Requirement set 1]

This requirement is not possible to meet since it requires reporting "after the occurrence of the associated call event." Some events take several seconds to even be detected in a switching systems (e.g., between the time a key is pressed

and the time the key is detected involves several queuing, transmission, and processing delays). On top of those delays processing for wireless mobility or intelligent network services may take several more seconds (sometimes 20 to 30 seconds) before the event is ready to be acted upon. This latter time may be the most convenient time to formulate and send the CDC message. Which time should the message use? How, when, and where are the precise events going to be defined? [Requirement set 1]

(e)(4) The delivery timing requirements shall be measured from when the reported event occurs at the IAP until the first bit of each event message begins transmission on the government procured facilities.

This requirement is not testable since the time of the "reported event" is not well defined. Any system can state that the event occurs immediately prior to message transmission and meet this requirement. [Requirement set 1]

(e)(5) The following messages shall be delivered to the demarcation point within no more than 5 seconds (99% probability): (i) Serving System Message; (ii) Feature Status Message; and (iii) Surveillance Status Message.

This requirement is onerous. Law enforcement will take some time (at least hours and perhaps days) to react to these messages. Because these messages may have to be generated from various administrative systems and then collected before transmission to law enforcement, it is likely that a 5 second requirement will require a complex and costly solution. [Requirement set 1]

ServingSystem messages report when an intercept subject moves to another market. Law enforcement's response may be to get another court order for the new market.

FeatureStatus messages are sent by various service network elements and administrative systems. Law enforcement's response is to change the number CCCs required or to get another court order for additional intercepts.

SurveillanceStatus messages may indicate possible problems in the transmission of surveillance information. Law enforcement's response is to localize the problem and get it fixed. The problem may be with the accessing service provider, with intermediate carriers and equipment, and with

the collection equipment. The accessing service provider is probably already aware of problems with its equipment due to system alarms.

(e)(6) To ensure that their equipment, facilities, or services are capable of providing information that enables law enforcement to correlate a set of call-identifying information messages from the CDC to a segment of call content received on a CCC, telecommunications carriers shall transmit a unique tag both in-band on the CCC and over the CDC in the CCOpen message.[5] Signaling on the CCC shall be used to inform law enforcement when call content is being delivered and to provide an event on the CCC with which the CCOpen message time stamp can be associated.

The basic premises of this requirement is misplaced. The telephone industry is able to switch millions of calls an hour without in-band call identifying information by using out-of-band common channel digital signaling. It is time for law enforcement to step into the digital age. It should be noted that by implementing either [requirement set 1] or [requirement set 2] above makes this requirement obsolete. [Requirement set 3]

The insertion of the identifying tags into the CCC increases the time required to deliver call content and may increase the requirements for capacity in order to not miss content on a series of serial calls made by an intercept subject. [Requirement set 3]

(A) The values of the CCOpen message TimeStamp parameter followed by the CCCSerialNumber parameter shall be transmitted using industry standard in-band signaling (i.e.,

---

[5] Although any set of messages from one call may share a common call identity, call identities will be reused frequently. In addition, several calls may be received sequentially over the same CCC within a short time period. Because network and collection equipment clocks are not synchronized and may differ by minutes or hours, an additional measure is needed for correlation.

While it is true that several calls may be delivered over a CCC in a short time period, each call is bracketed by a CCOpen and a CCClose message.

J-STD-025 does not allow call identities to be "immediately re-used."

(e)(2) requires that all messages referencing a common call have synchronized clocks. [2]

DTMF, MF, or FSK) on the CCC immediately before call content delivery.[6]

DTMF, MF or FSK precludes digital tagging of the CCC which may take less time. Injecting tones will require a guard band of 200 ms, 100 ms for each digit, followed by another guard band. As proposed the marker takes up to 25 digits (a time stamp takes 15 digits (YYYYMMDDHHMMSS.S, where YYYY is the year MMDD is the month and day, HHMM is the hour and minute, and SS.S is the seconds and tenth of seconds) followed by a 10-digit CCCIdentifier ($2^{32} \approx 4x10^9$)). To transmit the 25 digits and the guard bands will take almost 3 seconds. To take this amount of time requires that either call content be delayed or that some of the call content be possibly be obscured (in violation of J-STD-025. [Requirement set 3]

(B) The time stamp of the CCOpen message shall coincide with the start of delivery on the CCC. The CCCSerialNumber, appended to the CCOpen-message TimeStamp, shall be transmitted in-band on the CCC immediately prior to transmission of call content and enables that content to be directly associated with that CCOpen message.

Since the time stamp and CCCSerialNumber must be transmitted over the CCC and the time at which delivery occurs must follow the transmission of the time stamp, the time stamp must be for some future time and then the transmission of content may begin at that time. [Requirement set 3]

---

6 The time between call origination and answer generally allows sufficient time to transmit such a tag without overriding any portion of the call content.

This assumes a human is answering the phone and the phone is not near the human. This may not be true, especially for bookies taking a large volume of betting orders, modems, answering machines and automatic answer on some speakerphones. Overwriting any portion of the call content which is encrypted may prevent the recovery of any of the call content. This is why J-STD-025 has such a stringent requirement against obscuring call content (especially in the digital age).

(C) The CCOpen message as defined in J-STD-025, shall be modified to include the following parameter:

Table 5: CCC Serial Number Parameter (Addition to J-STD-025, Table 3)

CCC Serial Number	M	Uniquely correlates CDC messages to a particular call content transmitted on the CCC.

The insertion of a mandatory parameter violates the forward compatibility rules carefully crafted in J-STD-025. These rules allow changes to be made in the protocol without affecting existing systems. This parameter should be an Optional (O) parameter and should only be included if the CCC is tagged with a time stamp and CCCSerialNumber. [Requirement set 3]

(D) The CCOpen message initially shall be used to associate a particular call with a CCC on the dedicated circuit. If that call is later merged into another call and supported by another CCC, a Change message shall be delivered to maintain the association between the communication and the channel(s) on which it is delivered.

The first sentence is already required by J-STD-025 for circuit-mode call delivery.

The second sentence redesigns J-STD-025 which uses the Change message to report changes to the CallIdentities, rather than to report changes to the delivery of calls over a CCC, although the latter can be derived from the information in the Change message. Changing the triggers for the Change message will require redesign of the systems sending or receiving the Change message. If such a change is desired, it may have less impact to generate a new message for the purpose. [Requirement set 3]

(E) A serial number parameter shall be added to the CCOpen containing the following ASN.1 syntax definition:

```
CCOpen ::= SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
CHOICE {[3]     SEQUENCE OF CallIdentity, -- for circuit-mode intercepts
        [4]     PDUType,  -- for packet-mode intercepts},
        [5]     EXPLICIT CCCIdentity,
        [6]     CCCSerialNumber -- for correlation of CDC to CCC}
```

This requirement states in effect that only this message encoding can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

The insertion of a mandatory parameter violates the forward compatibility rules carefully crafted in J-STD-025. These rules allow changes to be made in the protocol without affecting existing systems. This parameter should be an Optional parameter and should only be included if the CCC is tagged with a time stamp and CCCSerialNumber. [Requirement set 3]

(F) The CCCSerialNumber parameter shall be a number that is assigned sequentially on a per CCC basis and shall not repeat within a 24-hour period. The CCCSerialNumber shall always be greater than zero, and shall be reset each day at midnight using local time.

CCCSerialNumber ::= VisibleString (SIZE (1..4))

This number is not very unique and does not catch CCC configuration errors. This specifies a particular design that requires a separate 32-bit counter for each CCC. This precludes designs that would use a common counter for all CCCs or a separate CCC for each CaseIdentifier. The use of a sequential number implies accountability requirements beyond that required for a simple numeric tag. [Requirement set 3]

Since the CCCSerialNumber is transmitted with time accurate to 100 ms and it is unlikely that there be two calls using the same CCC in the same 100 ms period, the time

stamp is sufficient to meet the requirements stated in this paragraph. [Requirement set 3]

It will be impossible for an intercept subject that makes 2 million calls in a single day to use all of the bits specified for this parameter. The subject would have to make 550 calls per second all day long from a single line. [Requirement set 3]

(f) *Surveillance Status Message.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of delivering a Surveillance Status message confirming that the interception software is working correctly and accessing the equipment, facilities, or services of the correct subscriber. The receipt of the Surveillance Status message over the CDC verifies that the CDC is operational.

Law enforcement has requested that telecommunication service providers provide them with messages that assure law enforcement that 1) the intercept is properly activated, 2) that the intercept is working, and 3) that the intercept link is working. 1) and 2) are the responsibility of the telecommunication service provider, but only up to the point of demarcation. They do this by adding instrumentation to their equipment to issue alarms for various failures and then monitor those alarms to correct the indicated problems. 3) is the responsibility of law enforcement with their "procured transmission equipment, facilities, or services." As such the SurveillanceStatus message is the responsibility of government, both in sending the message and in monitoring its proper receipt. Law enforcement has existing techniques to verify 1) and 2).

If all that they wanted was to verify CDC link operability, this would be a fairly simple thing to do. However, by including surveillance status and administrative status this capability becomes much more difficult to do and it opens the door for additional reporting requirements in the future (when there is no hope for reimbursement).

(f)(1) The SurveillanceStatus message shall be triggered and delivered whenever a surveillance is activated, updated, or deactivated.

Law enforcement has asked for more status information in the past and continues to ask for it in TR45.2. They want assurance that all IAPs used to access communication for a subject are properly activated and working. Due to the distributed nature of modern switching system, especially

wireless systems, this is a fairly difficult requirement. Either the message is generated by every IAP or the telecommunication service provider must ascertain that all IAPs are working and configured properly before sending the one message to law enforcement. This capability is complicated by the fact that capacity (expressed as CCC channel assignments) may be different for each intercept on a single subject or on different switches within a telecommunication service provider's network.

(f)(2) The SurveillanceStatus message shall also be sent periodically from once every hour to once every 24 hours for the duration of a surveillance. Updates concern changes to the number and identity of CCCs provisioned for the particular CaseIdentity.

(f)(3) The activate and update SurveillanceStatus messages shall report any call content channels assigned to the surveillance.

(f)(4) The SurveillanceStatus message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 6: SurveillanceStatus Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber. With the redefinition of subject and subscriber, there was a re-definition of CaseIdentity from its source in J-STD-025.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SurveillanceStatusType	M	Identifies the type of SurveillanceStatus report.
Provisioned CCCs	C	Included when call content channels are provisioned.

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

It may be useful for the SurveillanceStatus message to report the proper association of intercept subject identification with the CaseIdentity, even though the

transmission of such information may compromise the security and privacy of any unencrypted CDCs. This is needed to meet requirement stated in (f) to verify the "correct subscriber." J-STD-025 avoided the transmission of the intercept subject identification because of law enforcement's stated desire to use unencrypted CDC links even though it has been pointed out that access to the CDC links would prove valuable to criminal elements.

This message, if implemented, should include the automatic deactivation time to coincide with the expiration of the court order.

It may be more efficient to report all CaseIdentities associated with a particular CDC with a single message. This format requires one message for each CaseIdentity.

(f)(5) The SurveillanceStatus message shall adhere to the following ASN.1 syntax definition:

```
SurveillanceStatus :: = SEQUENCE {
                    [0]     CaseIdentity,
                    [1]     IAPSystemIdentity                    OPTIONAL,
                    -- Include to identify the system containing the IAP when the
                    -- underlying data carriage does not imply that system.
                    [2]     TimeStamp,
                    [3]     SurveillanceStatusType,
  provisionedCCCs   [4]     SEQUENCE OF EXPLICIT CCCIdentity     OPTIONAL}
```

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(f)(6) The SurveillanceStatus message shall include a SurveillanceStatusType parameter indicating the type of status reported in the following manner:

```
SurveillanceStatusType ::= ENUMERATED {
                    activated       (0),
                    updated         (1),
                    inProgress      (2),
                    deactivated     (3)}
```

This requirement states in effect that only this encoding of the parameter can be used and to change the parameter in

any way will require changing the final rule. As such, it is an over specification of a requirement.

This requirement is under specified because the terms are not defined.

(g) *Feature Status Message.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of delivering a Feature Status message that reports when a request is made by a subscriber, subject, or the service provider for the assignment, removal, activation, or deactivation of network-provided features, even when the subscriber, or a subject, modifies capabilities remotely through another phone or an operator unaware of an interception.[7] The FeatureStatus message shall report when a subscriber first gains or loses the ability to invoke, without delay, network-provided features that would affect the delivery to law enforcement of call content or call-identifying information related to that subscriber's equipment, facilities, or services. The FeatureStatus message is not required when a new capability is gained through the subscriber's terminal and is reported by other messages.

At a minimum this requires IAPs to be inserted in all places where profile information is stored reflecting the features and services subscribed by an intercept subject. However, due to the timing constraints and some additional requirements as

---

[7] *See generally* TIA/EIA/IS-41.5-C, at p. 150 [¶ 6.5.2.20] (February 1996) (description of "CallingFeatures Indicator").

This footnote is totally inappropriate. It is taken out of context and it usage does not imply the intended functionality here. The CallingFeatureIndicator is a parameter which is used to carry call control information from the HLR to the MSC serving a subscriber. It may be useful to extract the call waiting, three-way calling and conference indicators, but these alone do not meet the intended functionality. These indicators may be turned on or off for individual markets or even individual areas within a market. The true indicator for individual wireless subscribers is kept in the HLR or in associated SCPs.

The parameter also conveys some call forwarding information,. This information is present for compatibility with older systems as this information is no longer necessary with IS-41C or subsequent releases. The information about call redirection features for wireless subscribers, including variations of call forwarding, is kept in the HLR or associated SCPs.

to the meaning of a change, the IAPs may need to be inserted into various customer care and administrative systems.

The value of this message is undermined by service providers that allow the use of features on a demand basis, rather than a subscription basis. A subscriber is able to invoke three-way calling and incur a one-time charge rather than having to pay a monthly fee.

The first sentence requires all feature changes to be sent is inconsistent with the second sentence which limits the requirement to only the feature changes that may affect intercept delivery.

The phrase "an operator unaware of an interception" could be construed as a requirement on a service provider (A.K.A. an operator) that is not served an intercept order. This can occur when a subscriber roams to another system. The serving system is not aware of administrative changes made in the subscriber's home system. Likewise the home system is not aware of special features, such as roamer access port, which may be provided in the system providing service to the subscriber. There is not now, nor should there be, a requirement to exchange such administrative information between carriers. To protect the confidentiality of intercept information, all administrative changes would have to be exchanged between the intercept subject's home service provider and the serving system. [Of course what is an operator -- one who operates a system or someone working for operator services??]

The language used in the section is inconsistent. Common telecommunication terms associated with features are authorize, activate, register, and invoke (and the negated forms de-authorize, de-activate and de-register). A subscriber is authorized when allowed to use a feature. A feature is activated when it is enabled to be used. Some features require additional information such as a call forwarding forward-to number to be registered. A feature is invoked when it is actually used.

(g)(1) The FeatureStatus message shall report features that are assigned or removed as a result of service provider actions, or that are activated or deactivated remotely by using another's equipment, facilities, or services. The Feature Status message does not need to be reported when the assignment, activation, deactivation, or

removal of new features are detectable through other messages described in J-STD-025.

Assume that one must report authorizations and registrations only.. Individual activations, de-activations and invocations do not affect law enforcement's ability to receive intercepted call-identifying information or content.

(g)(2) The FeatureStatus message shall be triggered and delivered when the service provider assigns or removes and when the subject activates or deactivates the following features:

Assume that one must report authorizations and registrations only.. Individual activations, de-activations and invocations do not affect law enforcement's ability to receive intercepted call-identifying information or content.

(A) Call redirection features that affect the routing of calls, including all variations of call forwarding features (e.g., call forwarding busy and call forwarding unconditional);

(B) Multiple circuit features that affect the number of CCCs required to include all variations of multiparty features (e.g., call waiting, call hold, three-way calling, conference calling);

Call hold does not affect the number of CCCs in and of itself. What does affect the number of CCCs is the number of call appearances allowed for a given intercept subject.

(C) Features that affect surveillance trigger identities (e.g., number change feature); and

As written this is a fairly open-ended requirement. It has already been taken to mean subscriber requested directory number changes, directory number changes for NPA splits, and new service orders for wireless telephones. Some directory numbers changes appear as a delete of the old subscription information and the insertion of new subscription information in the switch. These systems would require the IAPs to be in the administrative systems or customer care systems where the reason for a change can be determined. These systems currently have no intercept capability and to add such a capability may further compromise the protection requirements of CALEA or require a more complex solution.

Detecting a new service order where an intercept subject activates a new service on an existing phone is nearly impossible to detect, since the service activation may be with another service provider and the intercept subject may be using a falsified identity.

This requirement is largely served by (D) below.

(D) Service suspend and service disconnect features.

(g)(3) The FeatureStatus message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 7: FeatureStatus Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber. With the redefinition of subject and subscriber, there was a re-definition of CaseIdentity from its source in J-STD-025.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
FeatureName	M	Identifies the feature or service.
FeatureModification	M	Identifies the type of successful feature change.
FeatureParties	C	Included when the feature involves association of parties to the feature.

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

This encoding requires a separate message for each feature event., Some user actions like programming a call forwarding number, may trigger two of these messages: one for registration and one for activation., It may be more efficient to send a set of redirection numbers without linking individual numbers to a feature name (because some features like one-number calling are quite complex and law enforcement has stated that their only use of this information is to obtain another surveillance order.)

Feature that use CCCs should be individually named so that law enforcement can ascertain the number of CCCs required for a particular intercept subject.

(g)(4) The FeatureStatus message shall adhere to the following ASN.1 syntax definition:

```
FeatureStatus :: = SEQUENCE {
                [0]     CaseIdentity,
                [1]     IAPSystemIdentity                   OPTIONAL,
                -- Include to identify the system containing the IAP  when
the
                -- underlying data carriage does not imply that system.
                [2]     TimeStamp,
featureName     [3]     VisibleString (SIZE (1..64) ),
                [4]     FeatureModification,
featureParties  [5]     SEQUENCE OF PartyIdentity       OPTIONAL
        -- included when feature usage records other party identities}
```

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(g)(5) The FeatureStatus message capability shall include a FeatureModification parameter that indicates only successful modifications to a subscriber's capabilities. The FeatureModification parameter is defined as follows:

```
FeatureModification ::= ENUMERATED {
        assignment                      (0),
        unassignment                    (1),
        activation                      (2),
        deactivation                    (3),
        changeOfAssociatedPartyIdList   (4)}
```

This requirement states in effect that only this parameter encoding can be used and to change the parameter in any way will require changing the final rule. As such, it is an over specification of a requirement.

Again only registrations and authorization should be required.

(h) *Continuity Check.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of delivering a continuity check in the form of an in-band signal (e.g., idle signal as defined in ANSI T1.403, Appendix D) or tone (e.g., DTMF C-tone) that will verify that CCCs between the carrier and a law enforcement agency are in working order.

A service provider must ensure that its equipment, facilities, and services work, but only up to the point of demarcation. Beyond the point of demarcation it is up to the government to procure and test such services. As such the continuity check is the responsibility of government, both in sending the signal and in monitoring its receipt since it is testing the transmission facilities. The marker requirements in (e)(2), (h)(2), and (h)(3) are an attempt to make this transmission testing tone the responsibility of the telecommunication service provider for dedicated facilities.

A continuity signal should be a signal that is distinguishable from other signals, so that the source of the signal can be ascertained. Using an idle signal is not appropriate because and idle signal may be generated by any number of pieces of equipment. Its presence would only indicate that the channel was connected some place in the network, not necessarily that it is connected to the right place. C-tone is a little better, but it would just indicate that the channel is connected to C-tone somewhere. This point has a high probability of being associated with electronic surveillance, but the connection may still be made as an administrative error (e.g., the wrong port or the wrong network element) or due to a switching or wiring error (e.g., the line was crossed with a surveillance CCC).

(h)(1) When dedicated circuits are used to support CCCs (nailed-up CCCs), the continuous signal or tone shall be applied to idle CCCs to verify continuity.

This requirement is only for dedicated circuit-mode CCCs. The require is incomplete as it does not specify the testing required for switched CCCs or for packet-mode CCCs using dedicated, packet-switched or circuit-switched delivery facilities.

The insistence of the use of dedicated circuit-mode facilities is an example of the slowness of law enforcement to accept the newer technologies.

(h)(2) When a CCC is selected for use and opened, the signal or tone shall be removed from the channel, enabling the transmission on the CCC coincident with the generation of the CCOpen message.

This requirement is inconsistent with requirements in (e) which require the insertion of a time stamp and a serial number before call content can be delivered over the CCC.

This requirement seems to be only for dedicated circuit-mode CCCs. The require is incomplete as it does not specify the testing required for switched CCCs or for packet-mode CCCs using dedicated, packet-switched or circuit-switched delivery facilities.

ISUP provides for a continuity test, but this test is provided on a link by link basis and not on an end-to-end basis as proposed here. Even if the test were end-to-end, it would not be coincident with the generation of the CCOpen message (at least not to within 100 ms). The built-in ISUP continuity technique for testing switched circuit facilities meets the requirements for testing the CCC, but it does not meet law enforcement's additional requirement for synchronizing the CCC and CDC.

(h)(3) The time stamp of the CCClose message shall coincide with the release of the CCC. This coincidence shall be indicated by the re-application of a continuous signal or tone on the CCC.

This requirement seems to be only for dedicated circuit-mode CCCs. The require is incomplete as it does not specify the testing required for switched CCCs or for packet-mode CCCs using dedicated, packet-switched or circuit-switched delivery facilities.

The insertion of the marker tones increases the time required to deliver call content and may increase the requirements for capacity in order to not miss content on a series of serial calls made by an intercept subject.

(i) *Dialed Digit Extraction.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of extracting the digits dialed by the subject following cut-through at the access point and delivering those digits to the law enforcement agency in a post-cut-through InBandDigits message containing the those digits.

Telecommunication carriers do no process DTMF digits following cut-through of a call. Law enforcement may get these digits from the transmission equipment that they use

(either as loop extenders or as dialed number receivers.) Such digits can be used to route the current call by using a subscribed service of another carrier such as an interexchange carrier or a pre-paid calling card service provider. Such digits can also be used to control customer premises equipment, such as answering machines, voice mail systems, PBXs, electronic banking, electronic brokerage, etc. CALEA requires that law enforcement use equipment to limit the digits delivered using dialed digit extraction to be call control digits. From a switching system perspective, it is easiest to presume that all post cut-through digits are used to control CPE and not call control. Otherwise one would have to check which access number was used, decided if that number provided a controllable telecommunication service (something beyond the control of the accessing system, and then only pass through the digits that could represent the called number. Any authorization codes would have to be stripped as they are not used to complete the call. After the call is cut-through by the accessed system, an event unknown to the accessing system, the digits again would have to be presumed to be controlling CPE. This is further complicated by the fact that some interexchange carriers allow the pound key "#" to be recall a dial tone from the accessed system, but only if the digit is sent for at least two seconds . Some "#" digits may be used control CPE, provided that the digit is sent for less than two seconds. It may be difficult or impossible for the accessing system to determine which down stream system interpreted the "#" digit. Again the safest solution, to meet the legal requirement, is to presume that the digit was processed by CPE and not by call processing.

The more technically correct solution is for law enforcement to obtain a surveillance order on the accessed interexchange carrier or pre-paid calling card service provider. Presumably the intercept subject has a subscription with them and only they know which digits were processed and how. Just because a DTMF digit was sent doesn't mean that it was interpreted, especially for short duration digits.

(i)(1) The InBandDigits message shall be delivered over the CDC and shall report subject inputs detected by the accessing switch (including any DTMF tones detected) that have partially or fully cut-through a call content path from the subject toward an associate. Inputs may be accumulated for up to thirty seconds or

until the maximum number of digits that can be carried by the InBandDigits message (32) is reached, whichever is earlier. Inputs accumulated in this manner shall be delivered in an InBandDigits message when an event precludes acting upon the input (e.g., call abandonment) or when the maximum number of digits that can be carried by an InBandDigits message is reached.

Digits used to originate a call have to be reported using the J-STD-025 message. Digits sent after origination, but prior to answer (and cut-through) are not interpreted by any public telecommunication system and therefore are not used by the accessing system for call processing.

(i)(2) The InBandDigits message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 8: InBandDigits Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber. With the redefinition of subject and subscriber, there was a re-definition of CaseIdentity from its source in J-STD-025.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
UserInput	M	Identifies specific user input when it is detected.

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(i)(3) The InBandDigits message shall adhere to the following ASN.1 syntax definition:

```
InBandDigits :: = SEQUENCE {
                [0]     CaseIdentity,
                [1]     IAPSystemIdentity              OPTIONAL,
                -- Include to identify the system containing the IAP  when
the
                -- underlying data carriage does not imply that system.
                [2]     TimeStamp,
                [3]     CallIdentity,
userInput       [4]     VisibleString (SIZE (1..32) )
        -- e.g., "12345" or "*123" or "#345"}
```

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(j) *Ceiling Limit on Number of Interfaces.* The total number of Interfaces used by the telecommunications industry to implement J-STD-025, and the standards defined in sections (a) through (i) hereof, shall not exceed five Interfaces for the CDC and five Interfaces for the CCC, respectively.

This requirement is unworkable, unless we prohibit consumer use of data or fax services. The number of interfaces may limit the number of physical delivery media used or the number of network layer packet protocols used, but other than that the number of permutations go way beyond the total of five requested here.

For example, a typical phone user today uses voice, fax and data. To deliver these to law enforcement using analog and digital facilities would require a minimum of six protocol stacks. But data modems and fax modems themselves negotiate different protocols for different speeds and compression services. Each combination is another protocol stack. Internet users use a variety of application layer protocols (e.g., FTP, HTML, SMTP) and each of these is another protocol stack. These must be multiplied by two as the internet packets are carried by either SLIP or PPP across the serial link established with the modem. It is easy for a consumer to use over twenty protocols in the course of a month.

This is a thinly veiled attempt to dictate and limit design.

(j)(1) An Interface includes a protocol sequence (i.e., the "Protocol Stack"). Each protocol layer in a Protocol Stack (i.e., the "OSI Layer") shall refer to an available industry-wide standard or widely-used protocol. An OSI Layer may be defined as a "null" layer, meaning that no protocol is used at that layer. Where appropriate (e.g., for the network layer), sub-layer protocols may be selected and identified. The following are the OSI Layers: Application, Presentation, Session, Transport, Network (Inter-network and Intra-network), Data, Link, and Physical.

(j)(2) Packet-mode CCCs may use any of the protocol stacks defined for either the CDC or CCC.

Since voice can be delivered over analog CCC facilities and packets cannot be delivered over analog CCC facilities, this requirement seems to require things that are not possible (at least data link layer framing is required for packet-mode delivery and that is not provided by a raw DS-0 or an analog facility that would be perfectly acceptable for a CCC).

(j)(3) The following table is included for explanatory purposes:

Table 9: Interface Protocol Example

OSI Layer	**CDC Protocol Stack (d)***					**CCC Protocol Stack (b)***				
	d^1	d^2	d^3	d^4	d^5	b^1	b^2	b^3	b^4	b^5
Application										
Presentation										
Session										
Transport										
Network: Inter-network										
Intra-network										
Data Link										
Physical										

*d = data; b = bearer

Exhibit 2

May 15, 1998

Mike Warren
Federal Bureau of Investigation
CALEA Implementation Section
14800 Conference Center Drive
Chantilly, VA 20153-045

Re: TIA Subcommittee TR45.2 ESS Ad Hoc Group
Request for Input

Dear Mr. Warren:

As you are aware, Subcommittee TR45.2 of the Telecommunications Industry Association ("TIA") is currently meeting under the auspices of the Enhanced Surveillance Service ("ESS") project. The goal is to create an industry standard that meets the enhanced surveillance requirements of the Department of Justice and the Federal Bureau of Investigation ("FBI") that go beyond those required by CALEA as reflected in J-STD-025.

While your letter of May 5, 1998 indicates that the FBI supports the nine "punch list" items as set forth in its petition to the Federal Communications Commission ("FCC"), it does not specifically endorse the requirements as outlined by the proposed regulations attached to the FBI's petition. From the inception of the ESS, the Subcommittee has repeatedly asked law enforcement to come forward with specifications for a definitive set of complete and concise requirements as a formal contribution to the ESS process. However, the FBI has chosen not to make a comprehensive submission thereby forcing industry to speculate as to the exact nature and extent of law enforcement's surveillance requirements.

When law enforcement explains the purpose and need for each requirement, industry can make an informed assessment and technical response as you saw yourself at the Tucson meeting. For example, there we agreed that law enforcement's desire for 5 standardized interfaces was impractical and undesirable. The same approach should be taken on each and every one of law enforcement's requirements.

However, industry continues to lack a clear and affirmative statement from law enforcement necessary to move forward in a productive and efficient manner. The ESS process is completely contribution driven. Therefore, the lack of a contribution of